WHAT IS CLAIMED IS:

1. A method for detecting an undesirable condition within a messaging network, comprising:

receiving a message;

identifying a source of the message;

if an entry in a database for the source has not been created, creating an entry in the database for the source, setting a source counter for the source to one, and creating a timestamp for the source;

if an entry in the database for the source has been previously created, incrementing the source counter by one and updating the timestamp;

comparing the source counter to a source threshold;

and when the source counter exceeds the source threshold over the course of a predetermined amount of time, triggering an alarm indicative of an undesirable condition.

2. The method of claim 1, further comprising:

identifying a destination for the message;

if an entry in the database for the destination has not been created, creating a sub-entry in the database for the destination and related to the source and setting a destination counter to one;

if an entry in the database for the destination has been previously created, incrementing the destination counter by one;

comparing the destination counter to a destination threshold; and

when the destination counter exceeds the destination threshold over the course of another period of time, triggering a destination alarm.

3. The method of claim 2, wherein the source threshold and the destination threshold comprise different values.

4. The method of claim 1, wherein the message is a short message system message.

5. The method of claim 1, wherein the messaging network allows for number portability.

6. The method of claim 1, wherein the messaging network comprises a wireless network.

7. The method of claim 1, wherein the source comprises a network user and the destination comprises an intermediary vendor.

8. A method for detecting a spam event in a messaging network, comprising:

monitoring message traffic in the messaging network;

for each new source address associated with a message, creating an entry in a database and setting a source address counter for that source address to a predetermined number and storing a timestamp corresponding to a time at which the message was received, and for a repeated source address, incrementing the source counter for the repeated source address and updating the timestamp;

comparing the source counter for a given source address to a source threshold;

and when the source counter exceeds the source threshold over the course of a predetermined amount of time, triggering an alarm indicative of a spam event.

9. The method of claim 8, wherein the message traffic comprises short message system messages.

10. The method of claim 8, wherein the messaging network comprises a wireless network.

11. The method of claim 8, wherein the method is performed by intermediary logically located between two telecommunication service providers.

12. A method of detecting a routing loop in a telecommunications network, comprising:

monitoring message traffic passing through an intermediary interconnecting at least two telecommunication service providers;

as message traffic passes through the intermediary, creating an entry in a database, setting a source address counter to a predetermined number and storing a timestamp corresponding to a time at which a first message passed through the intermediary, and incrementing the source address counter and updating the timestamp each time the first message again passes through the intermediary;

as message traffic passes through the intermediary, creating an entry in a database, setting a destination address counter to a predetermined number and storing a timestamp corresponding to a time at which a second message passed through the intermediary, and incrementing the destination address counter and updating the timestamp each time the second message passes through the intermediary;

comparing the source address counter and destination address counter for a given source address and a given destination address, respectively to a source address threshold and destination address threshold;

and when the source address counter and destination address counter, respectively exceed the source address threshold and destination address threshold over the course of a predetermined amount of time, triggering an alarm indicative of a routing loop.

13. The method of claim 12, wherein the source address threshold and the destination address threshold comprise different values.

14. The method of claim 12, wherein the message traffic comprises short message system (SMS) messages.

15. The method of claim 12, wherein the method detects routing loops caused by number portability.

16. The method of claim 12, wherein the telecommunications network comprises a wireless network.